CLAIMS

1. A method to avoid Internet fraud that is carried out by means of a multi-key card in which a business organization, one or more users from the business organization and an authorization center interact, the method comprising the following steps:

requesting the legitimizing of the business organization to operate with the authorization center;

checking out the business organization in a database of the authorization center, assigning the business organization an identification code, said data base being not available on the Internet;

sending a list of the users to the authorization center;

preparing a registry assigning each user an alias or NICK and loading the registry into the database so that the new users are accepted;

requesting a specific number of multi-key cards for users qualified to operate by means of a note or purchase order;

generating in the authorization center a set consisting of the specific quantity of multi-key cards, assigning a unique number to each set and another unique number to each card, relating this card number with the user's NICK;

distributing the multi-key cards to the corresponding user personally and the cards including a form that possesses an organic security seal where the user must sign and leave the user's fingerprint;

updating information for the delivery of cards and returning the information and the form to the authorization center;

qualifying the NICK of the user who has received the multi-key card, thus up-dating the cards qualified; and

confirming the qualification to the recognized user,

wherein the method further comprises the following steps to authenticate user identity through a web page:

entering an official legitimized web page, the business organization requests entry to a portal of the authorization center by means of a link and, once entered therein, enters the NICK and a PIN of the multi-key card;

converting via an authorization center network server the NICK and the PIN to a bar code, and sending the bar code to the database of the authorization center, the database being without an open connection where a laser reader connected to the database reads the data and verifies whether the NICK is authorized, whether the PIN entered belongs to that NICK and whether the PIN entered has not been used before, authorizing the operation if all the verifications are positive or denying the operation if any of the verifications is negative;

the server without open connection shows the verification result and sends the result to the network server, where another laser reader connected to the network server reads the verification result, authorizing or denying the user's requested operation.

2. The method to avoid Internet fraud according to claim 1, characterized in that the following step for the authentication of user identity by means of a call center comprises:

requesting legitimization as the user by means of a telephone call to the call center,

in response to the call center operator the user reports the user's NICK and a PIN code from the user's multi-key card, data that will be entered by the operator into the system that makes the verification of such data available,

the system verifies that the NICK is qualified, that the PIN corresponds to the NICK and that the PIN has not been used, authorizing the operation if all the verifications are positive or denying the authorization if any of the verifications is negative;

once the verification has been effected, giving a response to the request for legitimization of identity to the user who requests it by telephone and invalidates further use of the NICK and PIN combination for a future operation.

3. The method to avoid Internet fraud according to claim 1, wherein the PIN entered by the user has limited temporary validity.

4. The method to avoid Internet fraud according to claim 1, wherein the PIN entered by the user has a color determined as a function of the category of the user who holds the card.

5. The method to avoid Internet fraud according to claim 1, wherein the step of generating the multi-key cards includes the additional steps of:

generating the cards in sets and assigning to each a unique alphanumeric card code of X characters (numbers, capital letters and/or lower-case letters), the system verifying that there is no identical code in the database that are not available on the network;

generating a random alphanumeric code of variable length that will be utilized as a PIN;

repeating the operation as many times as the multi-key card contains PINs so the system can verify that a PIN is not repeated in the same card;

assigning the user NICK to the code of the multi-key card and keeping the information in the database, thus authorizing this multi-key card.

6. A multi-key card to avoid Internet fraud to be used in accordance with the method of claim 1, characterized as being of a usual size as that of a magnetic card, having imprinted thereon the user's NICK, a variable series of PINs (alphanumeric codes) hidden by a scratch-off type protective cover, a unique set code identifier issued by the authorization center printer at the time of generating a specific set of cards for the business organization, and a card code identifier consisting of a unique alphanumeric code of X characters which identify that multi-key card, relating the card to the user and to the PINs that the user is authorized to use; as well as that the front of the card may contain space for advertising.

7. The multi-key card according to claim 6, characterized in that the NICK is printed on the multi-key card and hidden by a scratch-off type protective cover.

8. The multi-key card according to claim 6, characterized in that the NICK is printed on a removable plastic strip.

9. The multi-key card according to claim 6, characterized in that the multi-key card is wrapped in shrink-seal cellophane.